

WHAT IS CLAIMED IS:

1 1. A method of authenticating a client to a server comprising:
2 generating a challenge at the client;
3 signing the challenge to form a signed challenge;
4 sending at least the signed challenge to the server;
5 verifying the signature of the challenge at the server; and
6 if the signature is verified, sending an indication of successful authentication to the
7 client.

1 2. The method of claim 1, wherein generating a challenge at the client
2 comprises generating a random number.

1 3. The method of claim 1, wherein generating a challenge at the client
2 comprises generating a sequential challenge.

1 4. The method of claim 1, wherein generating a challenge at the client
2 comprises generating a challenge based on data received from the server in a prior step.

1 5. The method of claim 4, wherein the data received from the server is a
2 challenge returned with a server response to a prior client query.

1 6. A method of using a one-time use card number for an online transaction,
2 comprising:

3 generating a one-time use card number at a user system;
4 authenticating the user system to an issuer system;
5 passing the one-time use card number from the user system to the issuer system;
6 passing the one-time use card number from the user system to a merchant system,
7 wherein the merchant system is programmed to present the one-time use card
8 number to the issuer system to effect a payment;
9 verifying the one-time use card number received from the merchant system with the one-
10 time use card number received from the user system; and
11 if the one-time use card number is verified, approving the transaction.

1 7. The method of claim 6, wherein passing the one-time use card number to
2 the issuer includes passing at least one other data element related to the online transaction.

1 8. The method of claim 7, wherein the at least one other data element is
2 selected from, or a function of, a user's account number, a user's private key, a transaction
3 time, a transaction amount, or a merchant ID.

10002847-103101